

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		10628729	
	Filing Date		2003-07-28	
	First Named Inventor	Anne Kirsten Eisentraeger		
	Art Unit	2136		
	Examiner Name	CARL G COLIN		
	Attorney Docket Number	MS1-1280US		

U.S.PATENTS								
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
/C.C./	1	6446205		2002-09-03	Lenstra			
If you wish to add additional U.S. Patent citation information please click the Add button.								
U.S.PATENT APPLICATION PUBLICATIONS								
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Published Application citation information please click the Add button.								
FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							<input type="checkbox"/>
If you wish to add additional Foreign Patent Document citation information please click the Add button.								
NON-PATENT LITERATURE DOCUMENTS								
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.						T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	10628729
Filing Date	2003-07-28
First Named Inventor	Anne Kirsten Eisentraeger
Art Unit	2136
Examiner Name	CARL G COLIN
Attorney Docket Number	MS1-1280US

/C.C./	1	BARRETO, PAULO S.L.M., et al., "Efficient Algorithms for Pairing-Based Cryptosystems," Universidade de Sao Paulo, Escola Politecnica, Sao Paulo (SP), Brazil & Computer Science Department, Stanford University, USA, pp. 1-16.	<input type="checkbox"/>
/C.C./	2	Boneh, et al., "Identity-Based Encryption from the Weil Pairing," SIAM J. COMPUT., Vol 32, No. 3, pp. 586-615, 2003 Society for Industrial and Applied Mathematics.	<input type="checkbox"/>
/C.C./	3	Boneh et al., "Short signatures from the Weil pairing," pp. 1-17.	<input type="checkbox"/>
/C.C./	4	Cantor, "Computing in the Jacobian of a Hyperelliptic Curve," Mathematics of Computation, Vol. 48, No. 177, January 1987, pp. 95-101.	<input type="checkbox"/>
/C.C./	5	Eisentrager, et al., "Fast Elliptic Curve Arithmetic and Improved Weil Pairing Evaluation," Topics in Cryptology, CT-RSA 2003, Marc Joye (Ed), pp. 343-354, LNCS 2612, Springer-Verlag, 2003.	<input type="checkbox"/>
/C.C./	6	FREY, GERHARD et al., "A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves," Mathematics of Computation, Vol. 62, No. 206, April 1994, pp. 865-874.	<input type="checkbox"/>
/C.C./	7	Galbraith, et al., "Implementing the Tate Pairing," Mathematics Dept., Royal Holloway, University of London, Egham, Surrey, UK & Hewlett-Packard Laboratories, Bristol, Filton Road, Stoke Gifford, Bristol, UK, pp. 1-14.	<input type="checkbox"/>
/C.C./	8	HESS, FLORIAN et al., "Two Topics in Hyperelliptic Cryptography," S. Vaudenay & A. Youssef (Eds.): SAC 2001, LNCS 2259, 2001, pp. 181-189.	<input type="checkbox"/>
/C.C./	9	JOUX, "The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems (Survey)," C. Fieker and D.R. Kohel (eds.): ANTS 2002, LNCS 2369, pp. 20-32, 2002 (Springer-Verlag Berlin Heidelberg 2002).	<input type="checkbox"/>
/C.C./	10	MENEZES, ALFRED J., et al., "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," (0018-9448/93 1993 IEEE, IEEE Transactions on Information...), 8 pages.	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	10628729
Filing Date	2003-07-28
First Named Inventor	Anne Kirsten Eisentraeger
Art Unit	2136
Examiner Name	CARL G COLIN
Attorney Docket Number	MS1-1280US

EXAMINER SIGNATURE

Examiner Signature	/Carl Colin/	Date Considered	06/17/2007
--------------------	--------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	10628729
Filing Date	2003-07-28
First Named Inventor	Anne Kirsten Eisentraeger
Art Unit	2136
Examiner Name	Colin
Attorney Docket Number	MS1-1280US

U.S. PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S. PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
/C.C./	1	20030081785	A1	2003-05-01	Boneh, et al.	
/C.C./	2	20030182554	A1	2003-09-25	Gentry, et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		10628729
Filing Date		2003-07-28
First Named Inventor	Anne Kirsten Eisentraeger	
Art Unit		
Examiner Name		
Attorney Docket Number	MS1-1280US	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
/C.C./	1	Frey, et al., "The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems," IEEE Transactions on Information Theory, Vol. 45, No. 5, July 1999, pp. 1717-1719.	<input type="checkbox"/>
/C.C./	2	Manoharmayum, "On the Modularity of Certain GL ₂ (F ₇) Galois Representations," Mathematical Research Letters 8, pp. 703-712 (2001).	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Carl Colin/	Date Considered	06/17/2007
--------------------	--------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.